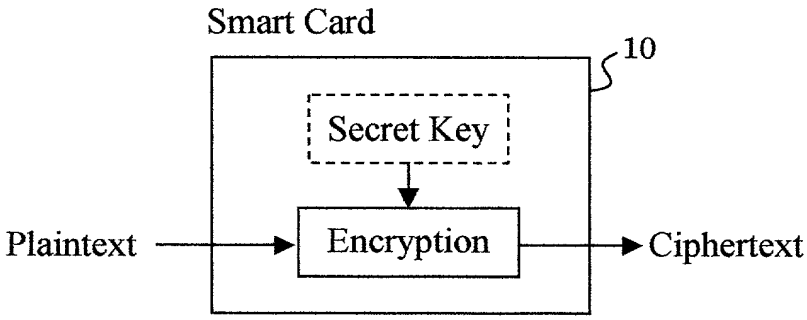


FIG. 1

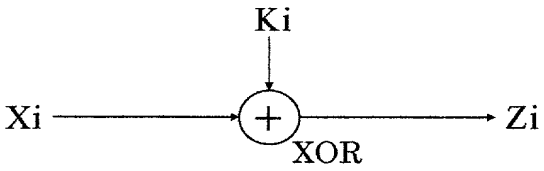


FIG. 2

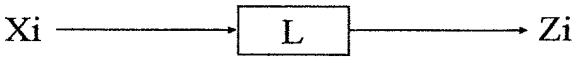


FIG. 3

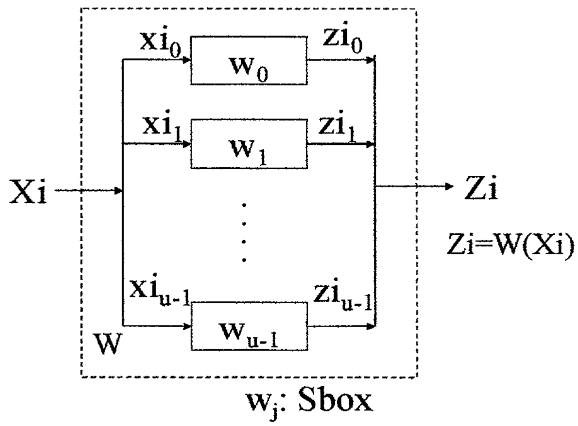


FIG. 4

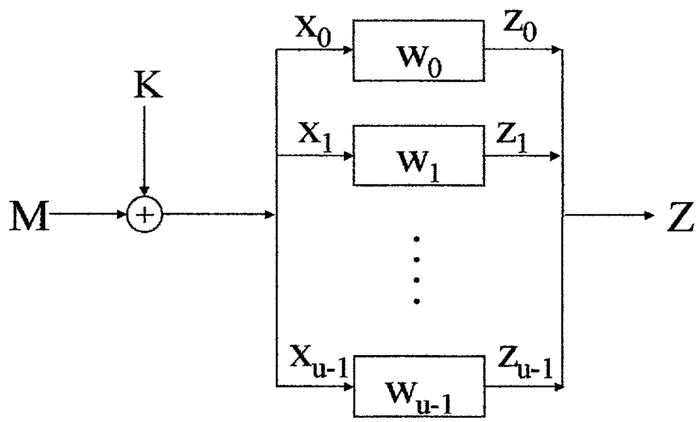


FIG. 5

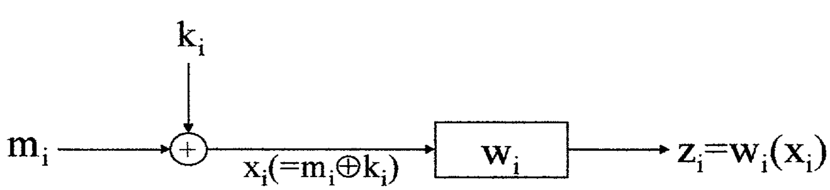


FIG. 6

FIG.7A

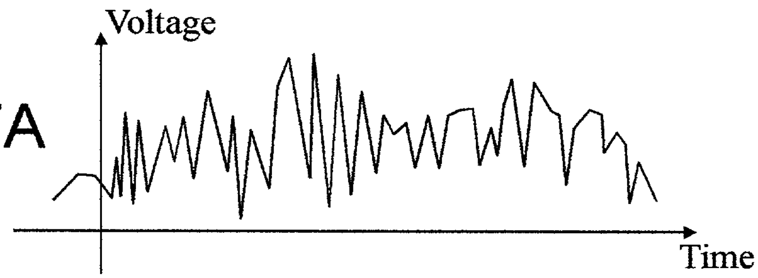


FIG.7B

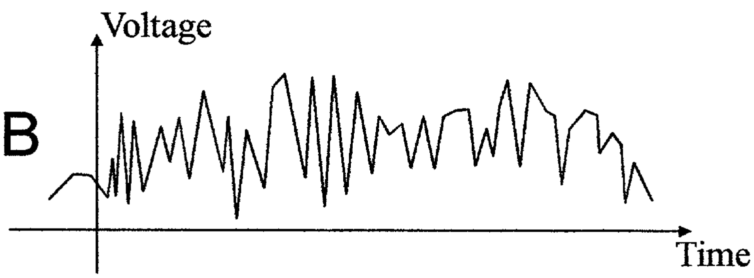


FIG.7C

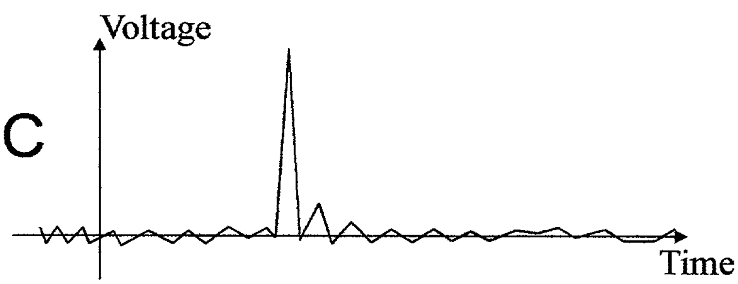
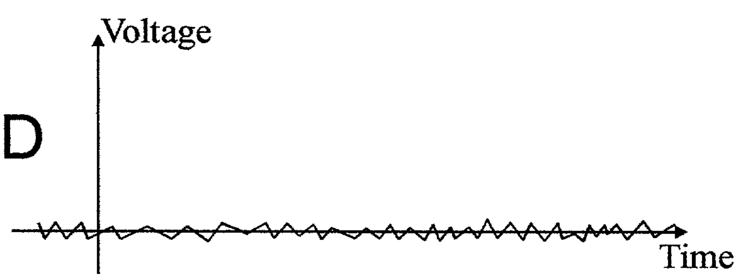


FIG.7D



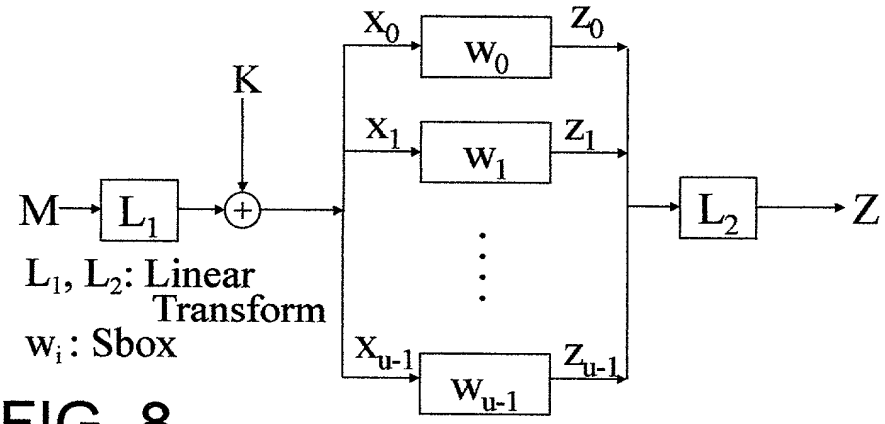


FIG. 8

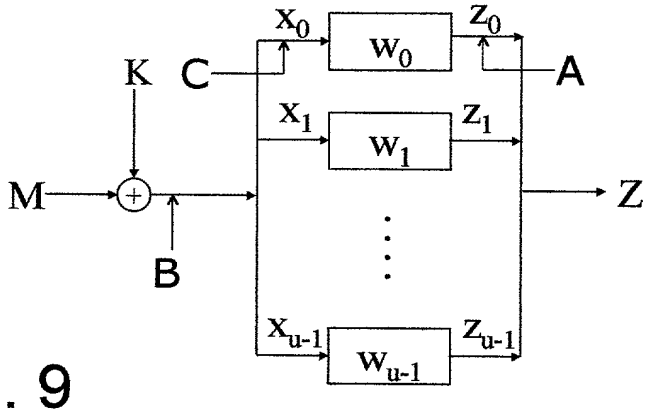


FIG. 9

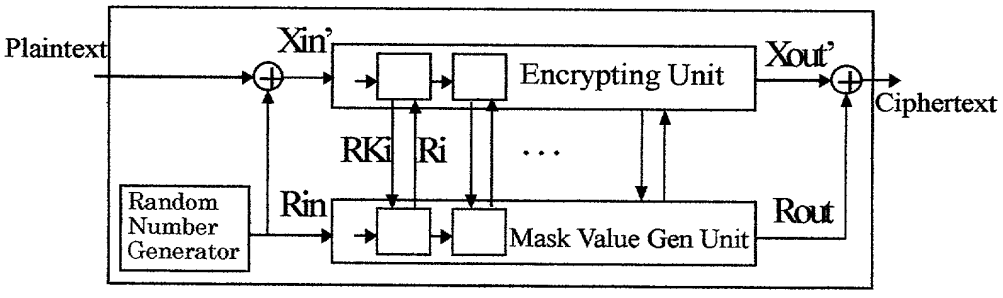
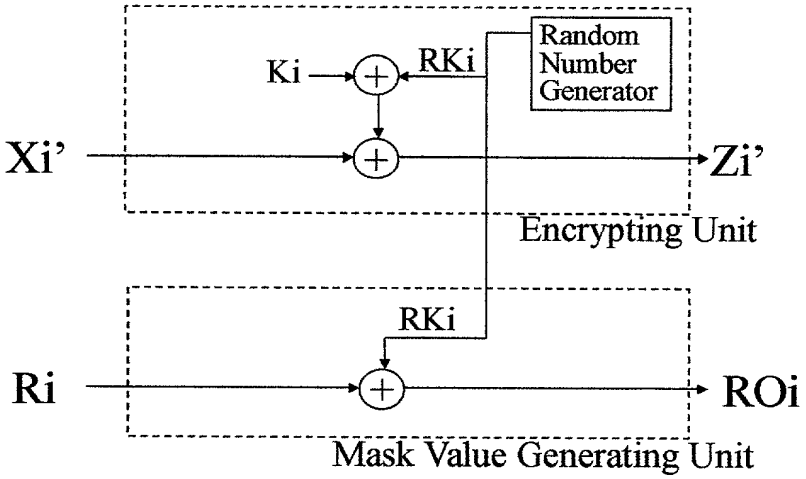


FIG. 10



Key XOR in Random Mask Value Method

FIG. 11

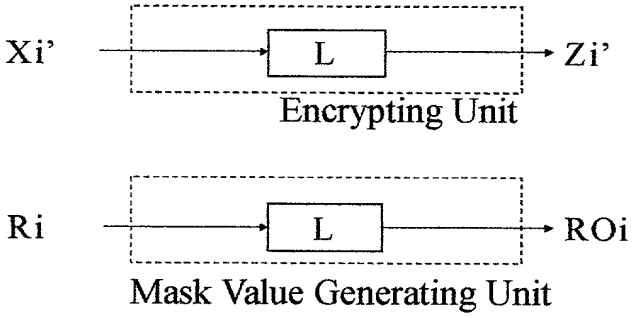


FIG. 12

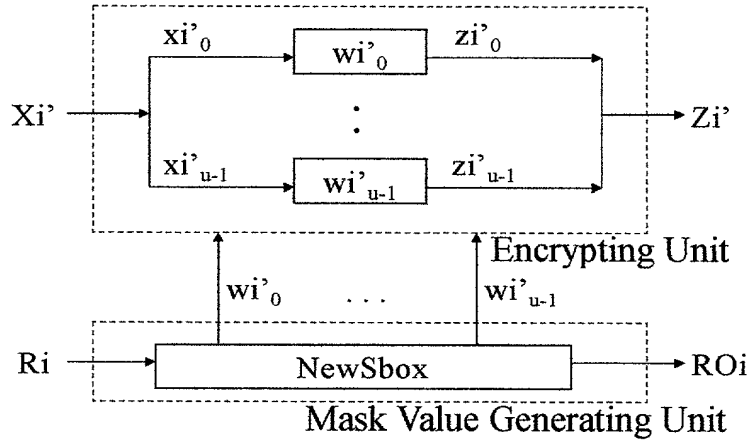
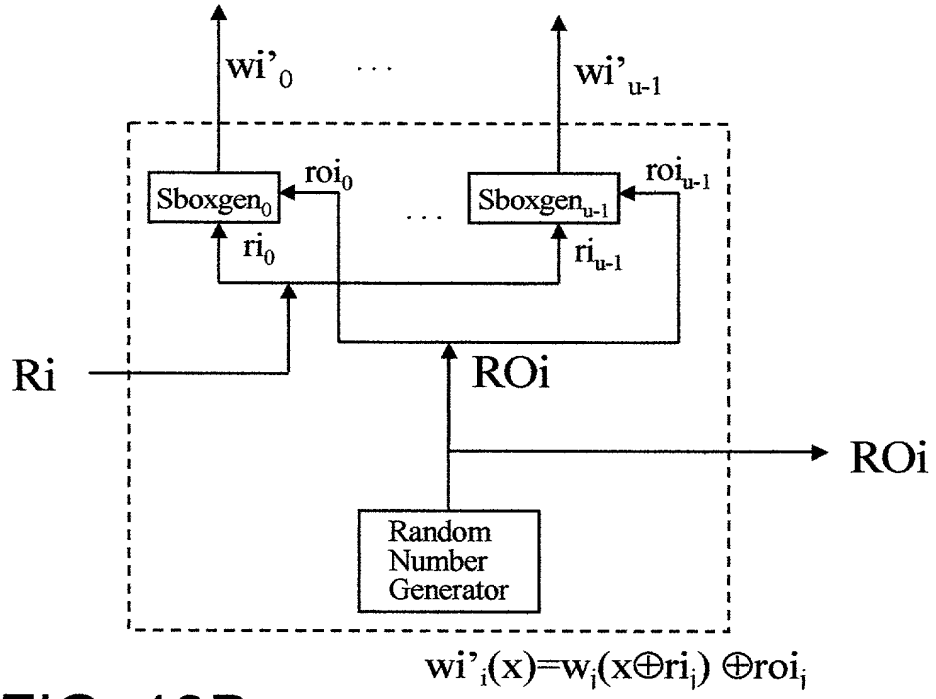
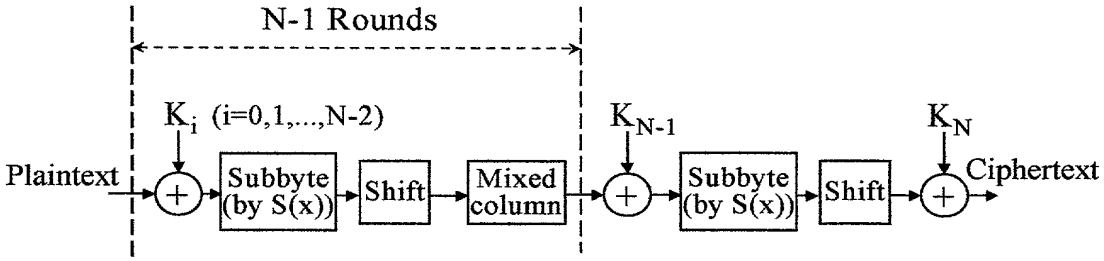


FIG. 13A



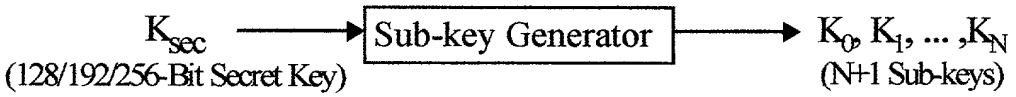
$wi'_i(x)=w_i(x \oplus ri_i) \oplus roi_i$

FIG. 13B



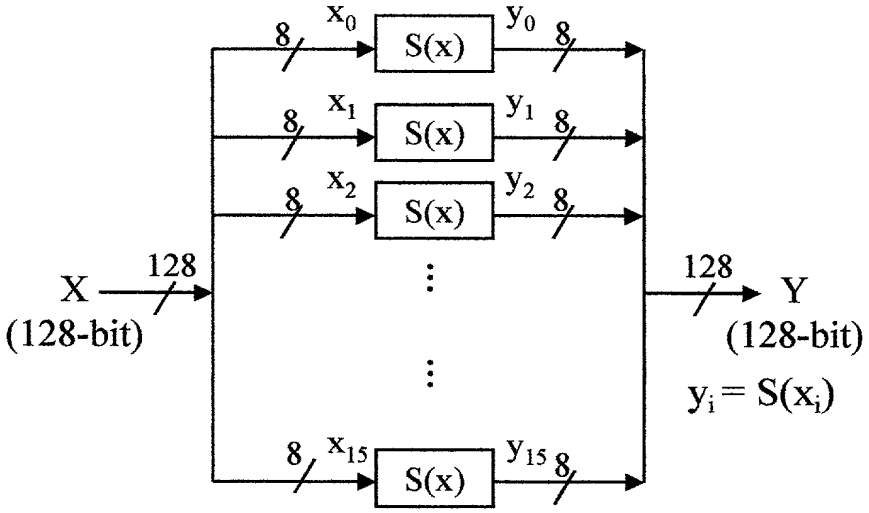
Conventional Rijndael Encryption

FIG. 14



Generation of Sub-keys in Rijndael Encryption

FIG. 15



Subbyte

FIG. 16

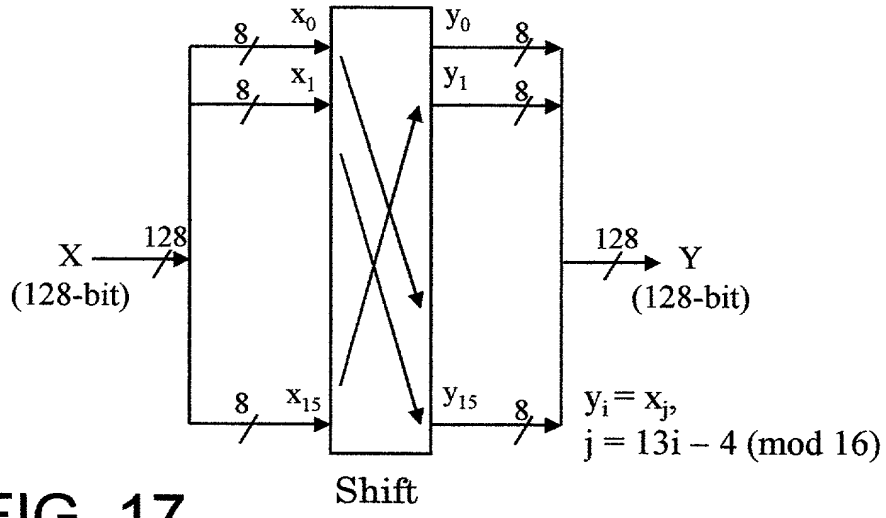


FIG. 17

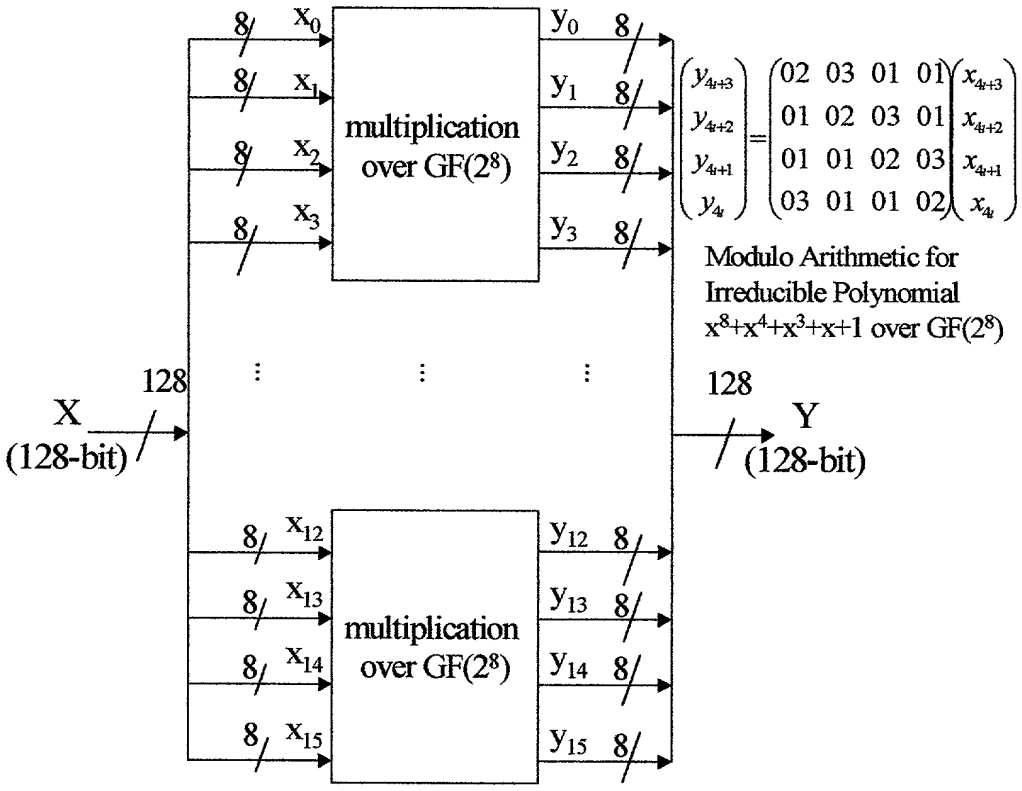


FIG. 18

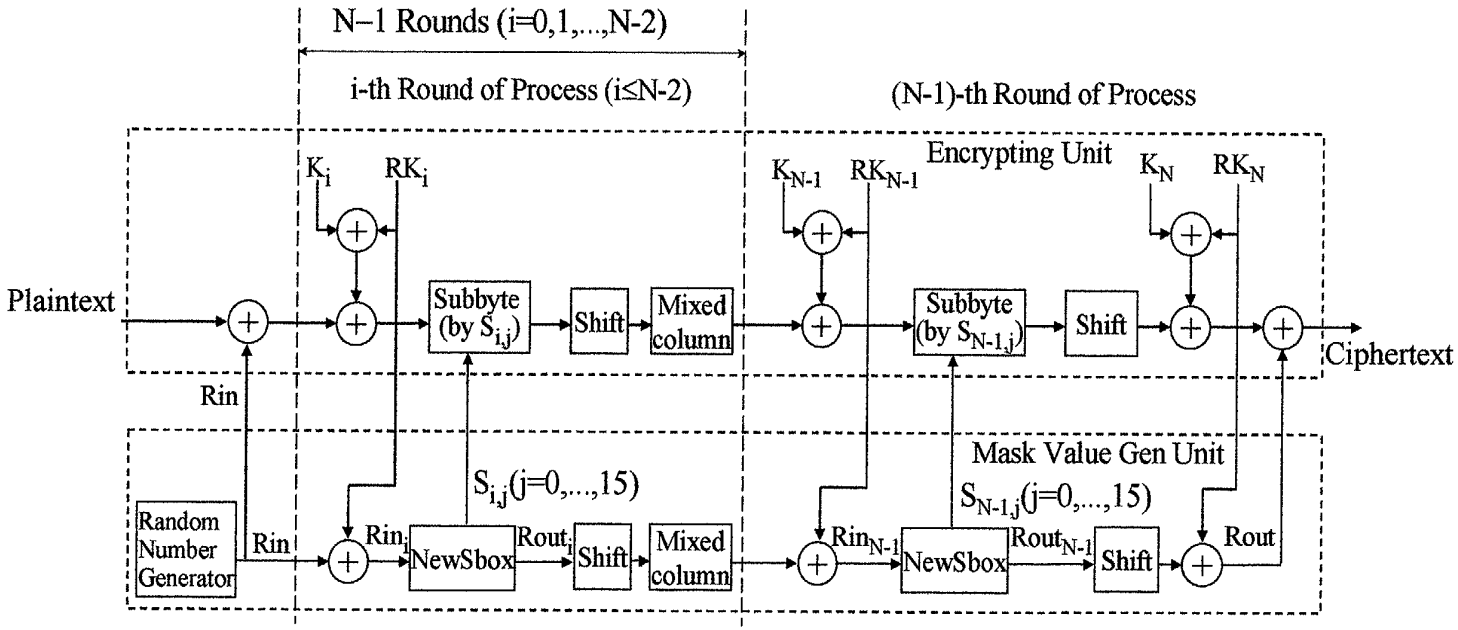
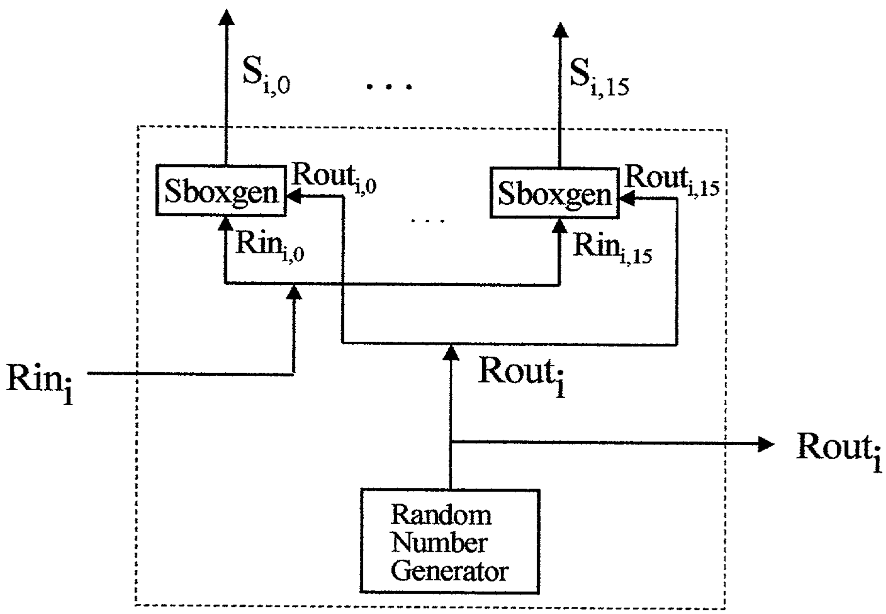

N−1 Rounds (i=0,1,...,N-2)
i-th Round of Process (i≤N-2)
(N-1)-th Round of Process
Encrypting Unit
Plaintext
Ciphertext
K_i
RK_i
Subbyte (by $S_{i,j}$)
Shift
Mixed column
K_{N-1}
RK_{N-1}
Subbyte (by $S_{N-1,j}$)
Shift
K_N
RK_N
Rin
Mask Value Gen Unit
$S_{i,j}$(j=0,...,15)
$S_{N-1,j}$(j=0,...,15)
Random Number Generator
Rin
Rin_i
NewSbox
$Rout_i$
Shift
Mixed column
Rin_{N-1}
NewSbox
$Rout_{N-1}$
Shift
Rout

FIG. 19



Sboxgen Generates Sbox, $S_{i,j}$, such that $S_{i,j}(x)=S(x \oplus Rin_{i,j}) \oplus Rout_{i,j}$

NewSbox

FIG. 20

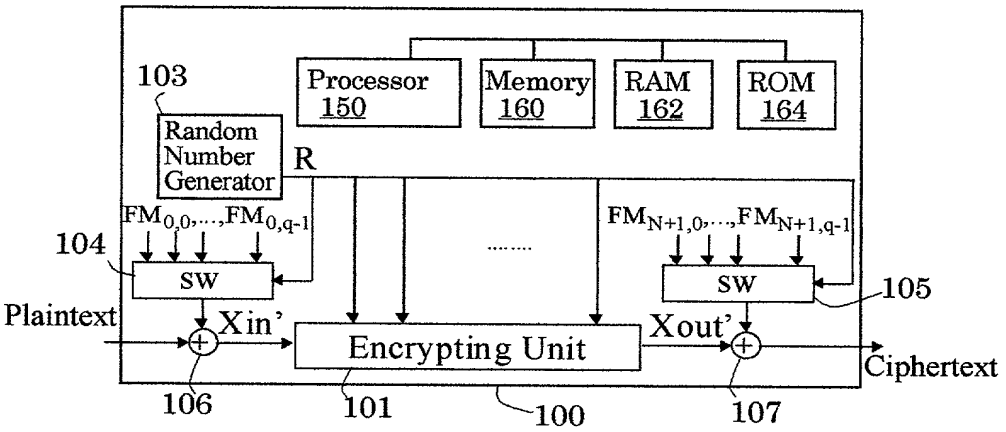
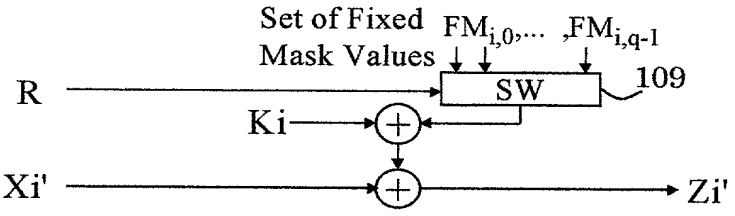
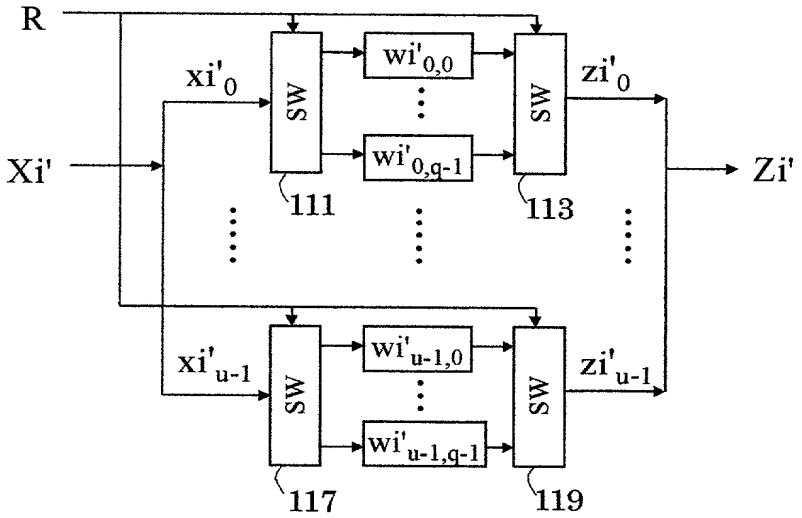


FIG. 21



Key XOR

FIG. 22



Nonlinear Transform

FIG. 23

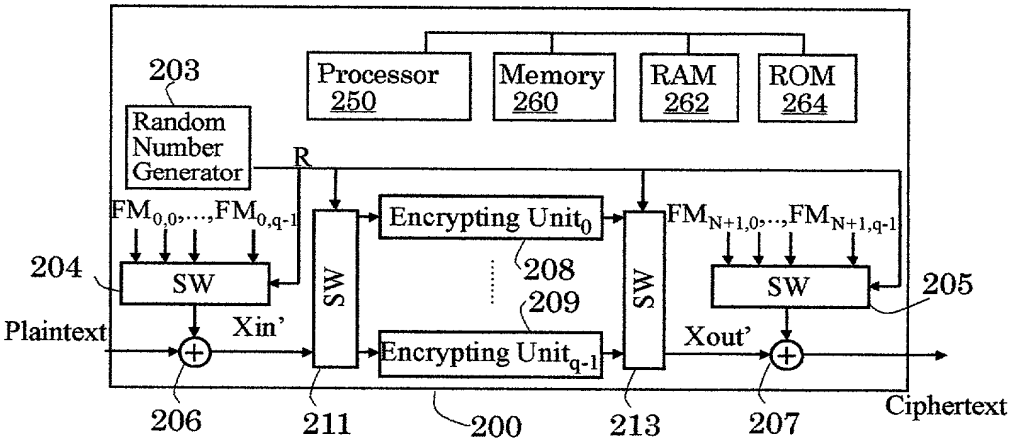


FIG. 24

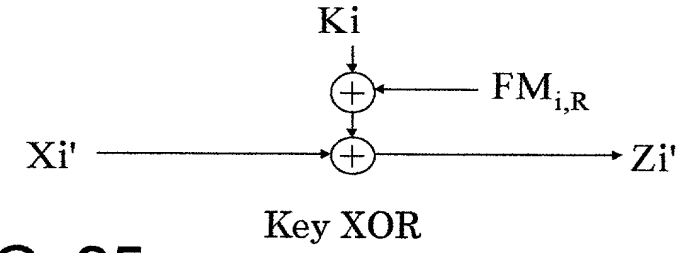


FIG. 25

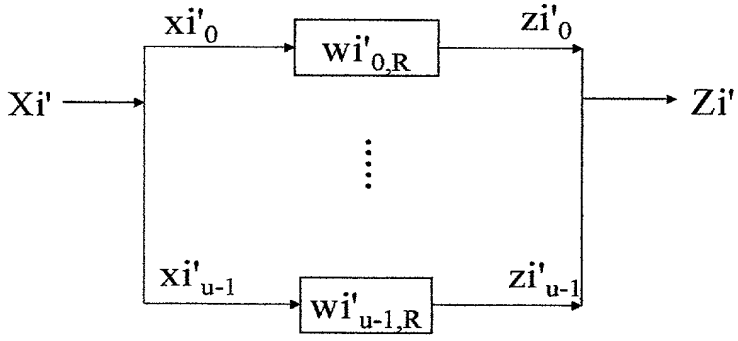


FIG. 26

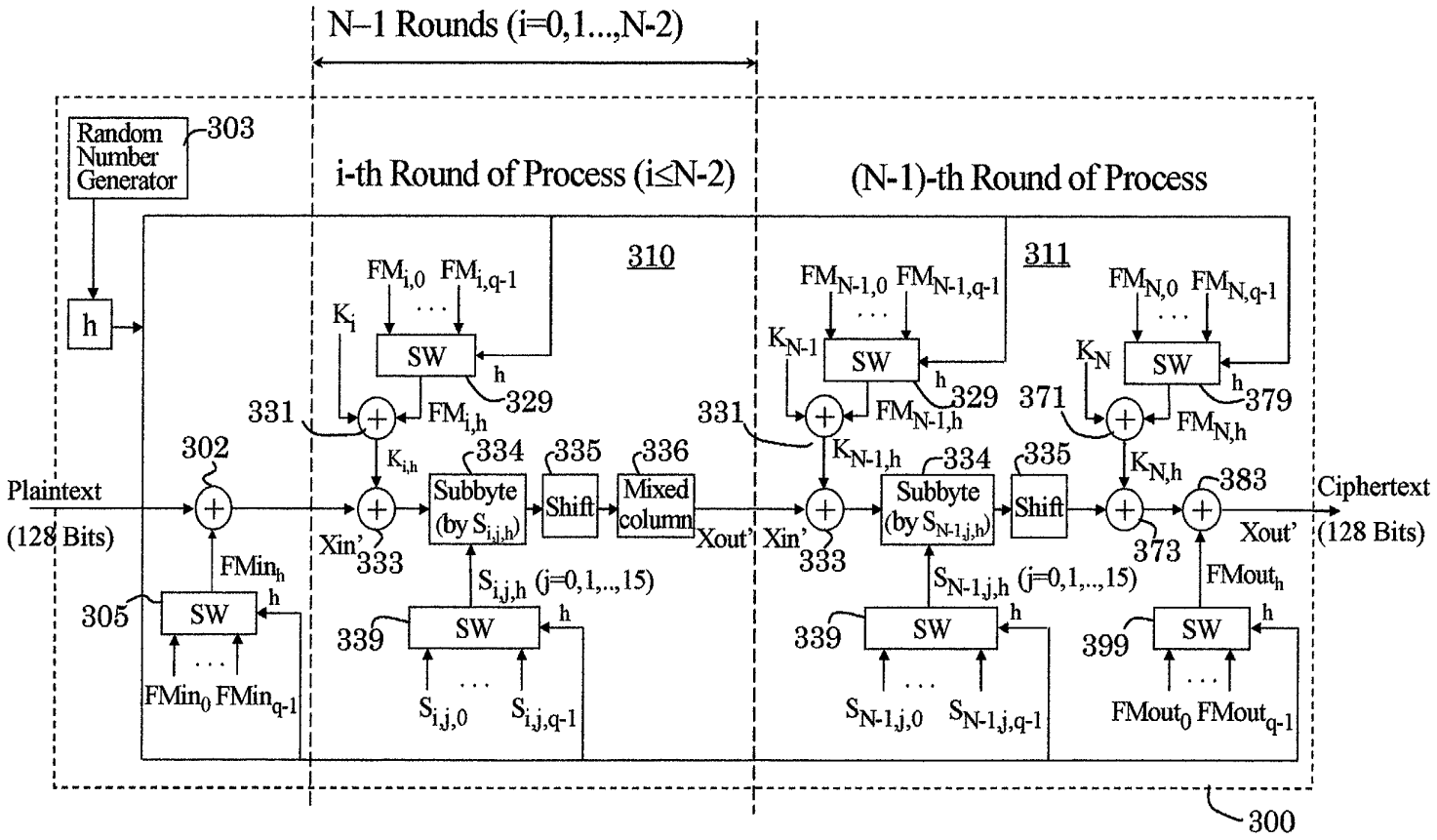
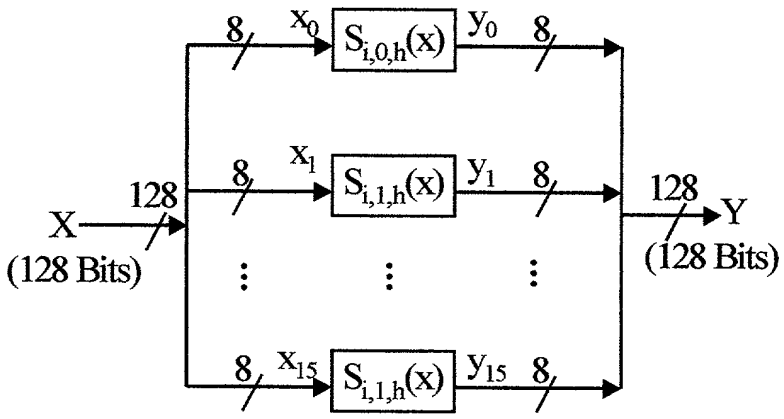

N−1 Rounds (i=0,1...,N-2)
Random Number Generator
303
i-th Round of Process (i≤N-2)
(N-1)-th Round of Process
310
311
h
SW
329
331
334
335
336
Subbyte (by S_{i,j,h})
Shift
Mixed column
Xin'
Xout'
333
302
Plaintext
(128 Bits)
FMin_h
305
FMin_0 FMin_{q-1}
S_{i,j,h} (j=0,1,..,15)
339
S_{i,j,0} S_{i,j,q-1}
FM_{i,0} FM_{i,q-1}
K_i
FM_{i,h}
K_{i,h}
FM_{N-1,0} FM_{N-1,q-1}
K_{N-1}
FM_{N-1,h}
K_{N-1,h}
S_{N-1,j,h} (j=0,1,..,15)
S_{N-1,j,0} S_{N-1,j,q-1}
FM_{N,0} FM_{N,q-1}
K_N
FM_{N,h}
K_{N,h}
371
379
373
383
399
FMout_h
FMout_0 FMout_{q-1}
Ciphertext
(128 Bits)
300

FIG. 27



$S_{i,j,h}(x)=S(x \oplus c_{i,j,h}) \oplus d_{i,j,h}$

S(x): Sbox in Conventional Rijndael Process

Subbyte

FIG. 28

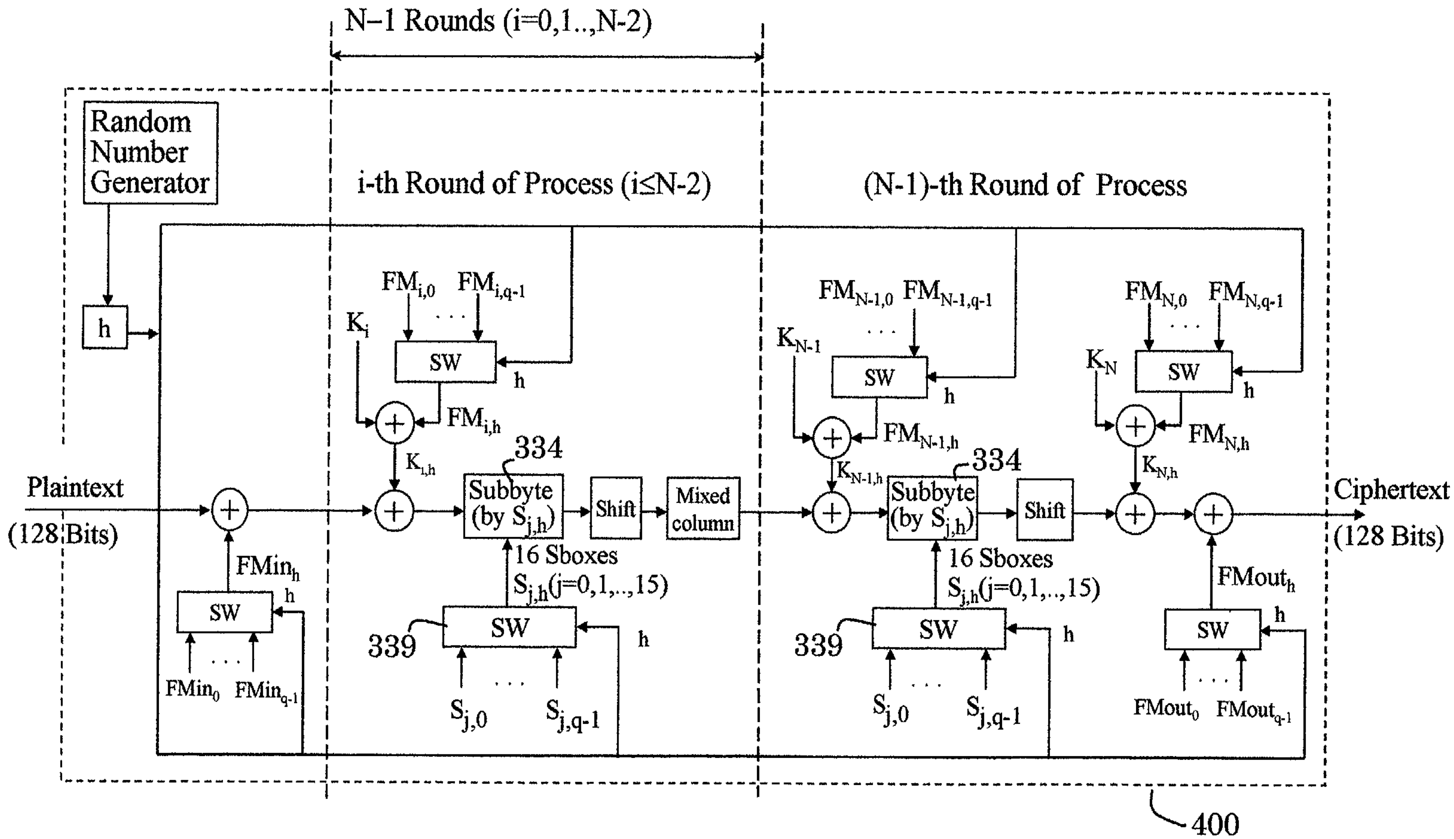

N−1 Rounds (i=0,1..,N-2)
Random Number Generator
h
i-th Round of Process (i≤N-2)
(N-1)-th Round of Process
Plaintext
(128 Bits)
FMin_h
SW
FMin_0 FMin_q-1
K_i
FM_i,0 FM_i,q-1
SW
FM_i,h
K_i,h
334
Subbyte (by S_j,h)
Shift
Mixed column
16 Sboxes
S_j,h(j=0,1,..,15)
339
SW
S_j,0 S_j,q-1
K_N-1
FM_N-1,0 FM_N-1,q-1
SW
FM_N-1,h
K_N-1,h
334
Subbyte (by S_j,h)
Shift
16 Sboxes
S_j,h(j=0,1,..,15)
339
SW
S_j,0 S_j,q-1
K_N
FM_N,0 FM_N,q-1
SW
FM_N,h
K_N,h
FMout_h
SW
FMout_0 FMout_q-1
Ciphertext
(128 Bits)
400

FIG. 29

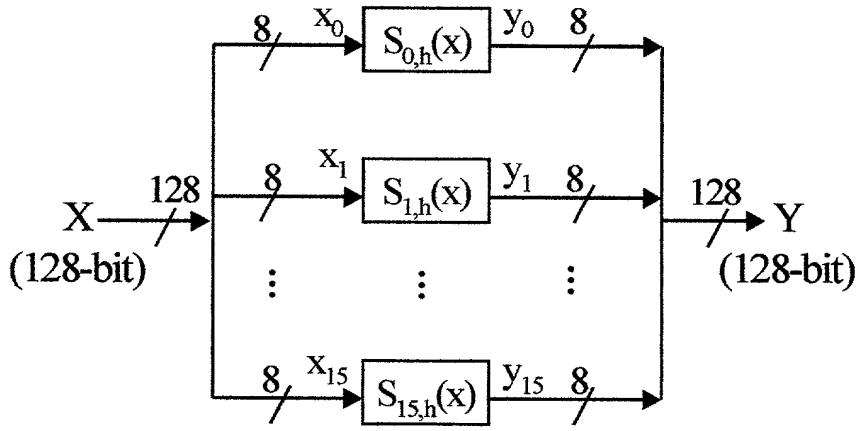


FIG. 30

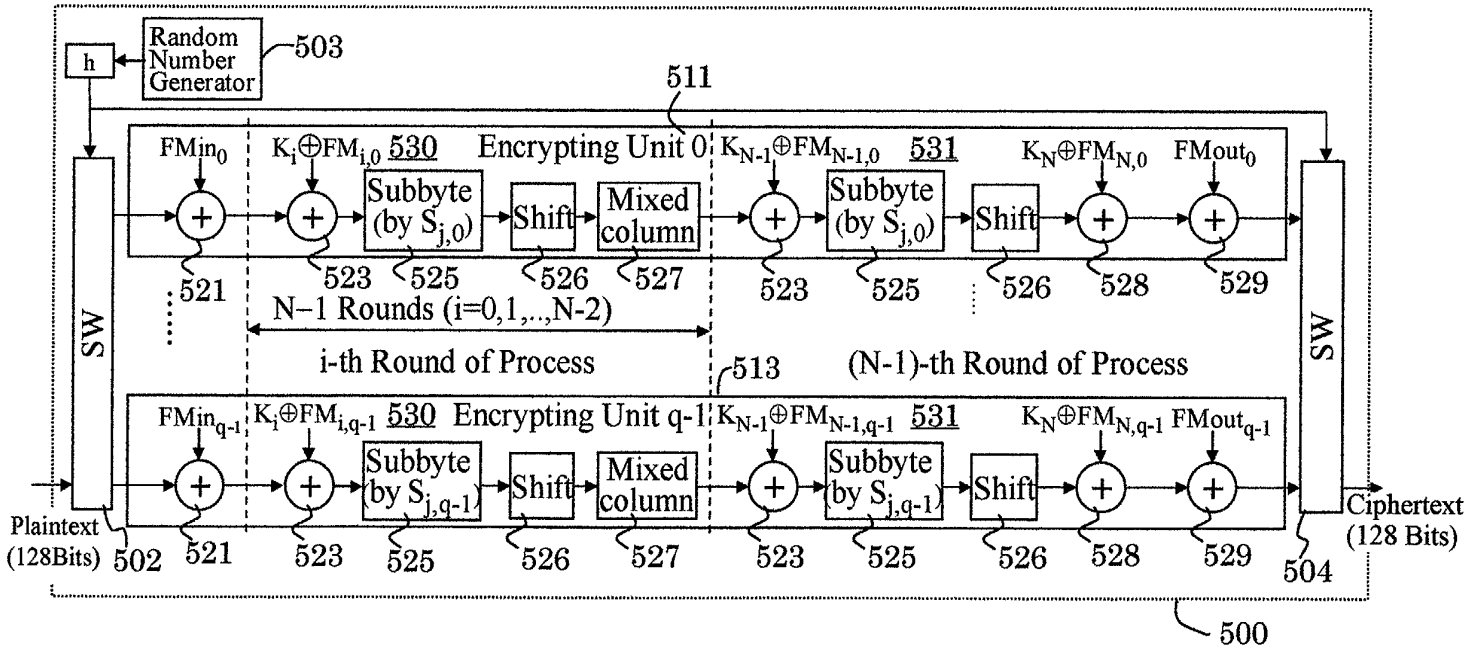

h
Random Number Generator
503
511
SW
FMin0
Ki⊕FMi,0 530
Encrypting Unit 0
KN-1⊕FMN-1,0 531
KN⊕FMN,0
FMout0
Subbyte (by Sj,0)
Shift
Mixed column
521
523
525
526
527
528
529
N−1 Rounds (i=0,1,..,N-2)
i-th Round of Process
513
(N-1)-th Round of Process
FMinq-1
Ki⊕FMi,q-1 530
Encrypting Unit q-1
KN-1⊕FMN-1,q-1 531
KN⊕FMN,q-1
FMoutq-1
Subbyte by Sj,q-1
Plaintext (128Bits)
502
504
Ciphertext (128 Bits)
500

FIG. 31

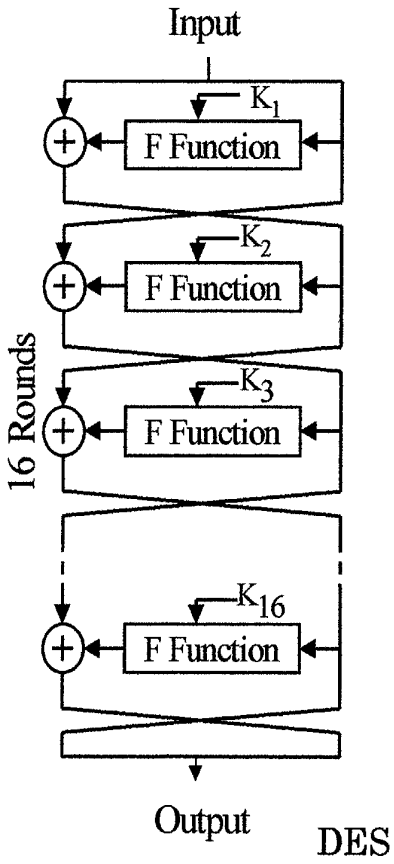
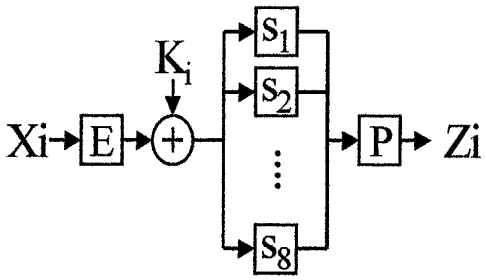


FIG. 32A



F Function

E P : Linear Transform

S1....S8 : Table of Nonlinear Transform

FIG. 32B

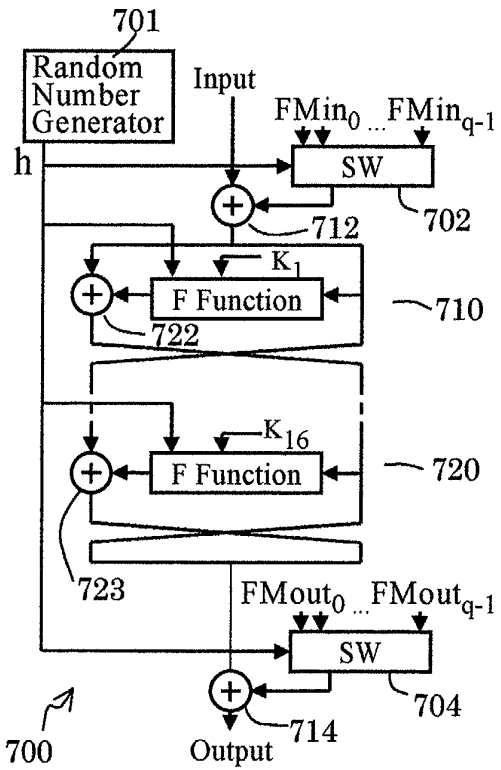
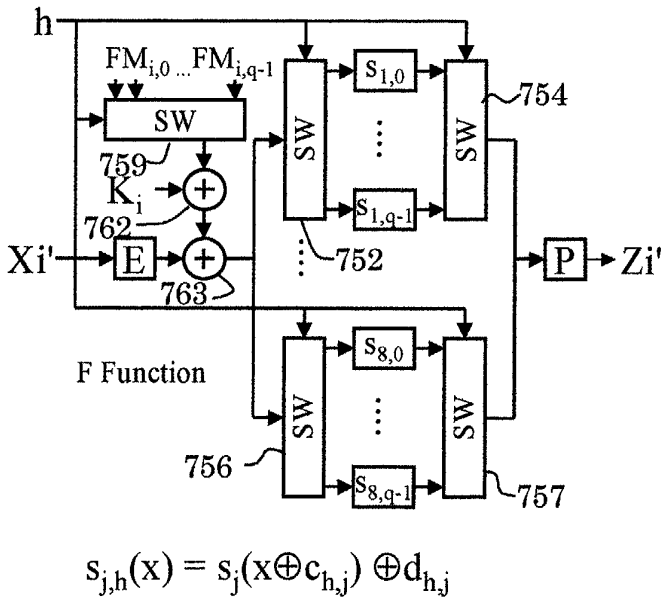


FIG. 33A



$$s_{j,h}(x) = s_j(x \oplus c_{h,j}) \oplus d_{h,j}$$

FIG. 33B

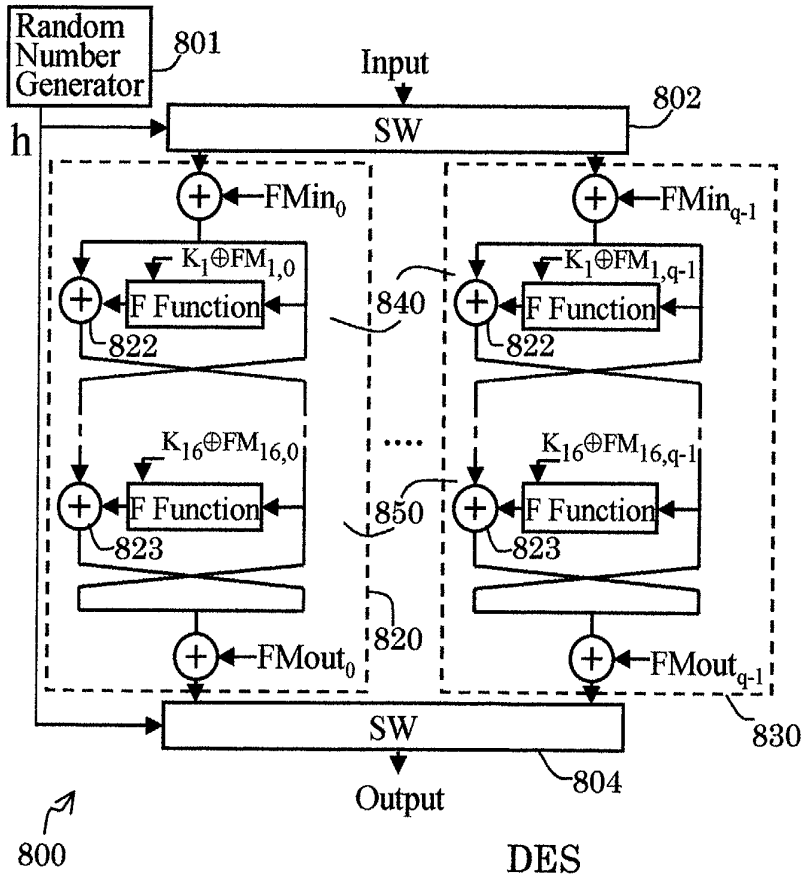


FIG. 34A

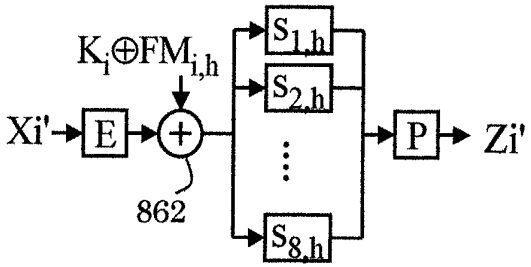
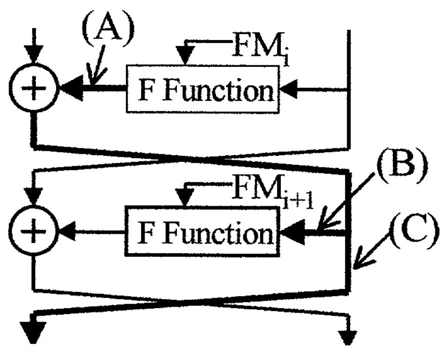
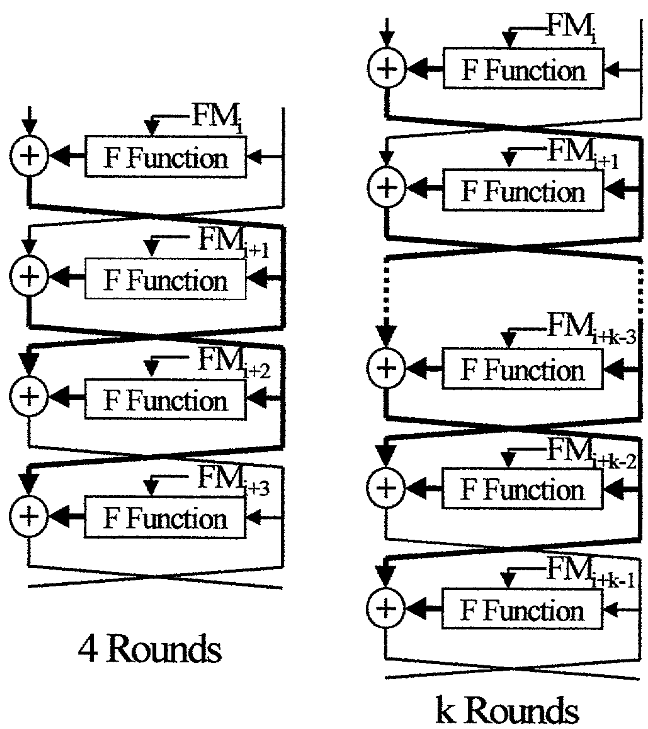


FIG. 34B



Propagation of Mask in Feistel Encryption

FIG. 35



Paths from Mask Value Generation to Cancellation in Feistel Encryption Device

FIG. 36